EQUIPMENT AND SYSTEM FOR CIPHER COMMUNICATION AND CIPHERING DEVICE

Patent number:	JP9018469
Publication date:	1997-01-17
Inventor:	YAMAMOTO TAKAHISA
Applicant:	CANON INC
Classification:	
- international:	H04L9/16; H04L9/22
- european:	
Application number:	JP19950165932 19950630
Priority number(s):	

Abstract of **JP9018469**

PURPOSE: To set the proper ciphering system by a transmitter and a receiver in a ciphering communication network.

CONSTITUTION: A terminal 10 for communication is provided with ciphering devices 11 performing ciphering and decoding which are different in ciphering systems, a selection means 14 selecting one of the ciphering devices 11 and a key generation/selector 13 generating the ciphering key according to the selection. The ciphering system which is suitable for the communication is discussed, determined and selected with the terminal 10 for communication on an opposite side. Therefore, the ciphering system having the ciphering intensity according to the secrecy required for information to be communicated is set.

Data supplied from the ***esp@cenet*** database - Patent Abstracts of Japan

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－18469

(43)公開日　平成９年(1997)１月17日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/16			Ｈ０４Ｌ	9/00	６４３	
	9/22					６５５	C5-6

審査請求　未請求　請求項の数９　ＯＬ　（全 14 頁）

(21)出願番号　特願平7－165932

(22)出願日　平成７年(1995)６月30日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　山本　貴久
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

(74)代理人　弁理士　國分　孝悦

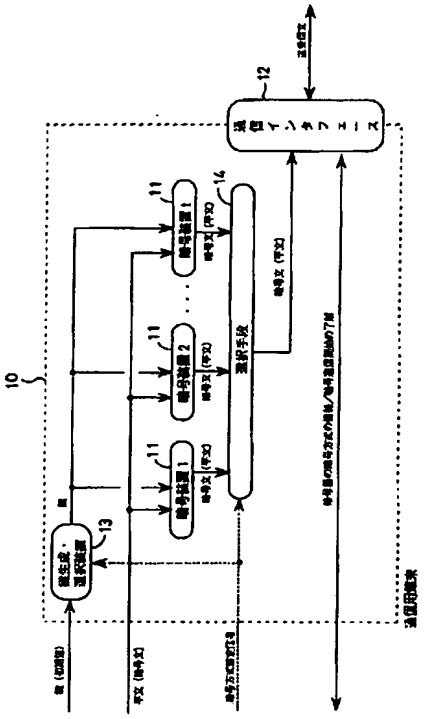
(54)【発明の名称】　暗号通信装置、システム及び暗号装置

(57)【要約】

【目的】　暗号通信ネットワークにおいて送受信者が適切な暗号方式を設定できるようにする。

【構成】　通信用端末１０には、それぞれ暗号方式の異る暗号化及び復号を行う暗号装置１１、暗号装置１１の１つを選択する選択手段１４、その選択に応じて暗号の鍵を生成する鍵生成・選択装置１３が設けられ、相手側の通信用端末１０とその通信に適した暗号方式を互いに打合わせをして決定し、選択できるようにする。

【効果】　通信する情報に要求される機密性に応じた暗号強度を有する暗号方式を設定することができる。



1

【特許請求の範囲】

【請求項１】　それぞれ送信データの暗号化及び受信暗号化データの復号を行い、互いに通信を行う複数の通信手段と、

上記通信手段に設けられ、複数の暗号化方式の１つを選択する選択手段とを備えた暗号通信装置。

【請求項２】　上記通信手段に設けられ、上記選択手段が選択した暗号化方式に対応した鍵を生成する鍵生成手段を備えた請求項１記載の暗号通信装置。

【請求項３】　上記通信手段に設けられ、上記送信データの暗号化処理時に上記鍵生成手段で生成される鍵を随時更新させる更新手段を備えた請求項２記載の暗号通信装置。

【請求項４】　上記通信手段に設けられ、上記選択手段が選択する暗号化方式を、互いに通信を行うことにより決定する決定手段を備えた請求項１記載の暗号通信装置。

【請求項５】　上記鍵生成手段で用いるアルゴリズムとして、計算量的に安全な疑似乱数生成のアルゴリズムを用いることを特徴とする請求項２記載の暗号通信装置。

【請求項６】　上記計算量的に安全な疑似乱数生成アルゴリズムとして２乗型疑似乱数生成アルゴリズムを用いることを特徴とする請求項５記載の暗号通信装置。

【請求項７】　複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、

動作モードを指定するモード指定手段とを備え、

上記暗号化手段は、指定されたモードに応じて暗号化方式を選択することを特徴とする暗号装置。

【請求項８】　複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、

セキュリティランクを指定する指定手段とを備え、

上記暗号化手段は、指定されたセキュリティランクに応じて暗号化方式を選択することを特徴とする暗号装置。

【請求項９】　ネットワーク上の複数端末間で暗号化されたデータの通信を行うとともに、暗号化方式を選択し得るようにした暗号通信システムであって、

所定の端末装置により指定された暗号化方式を他の端末装置により変更する場合に、上記所定の端末装置側の承諾を必要とすることを特徴とする暗号通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、データを秘匿するためにデータを暗号化して通信を行う暗号通信装置、システム及びそれに用いる暗号装置に関するものである。

【０００２】

【従来の技術】近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛生通信の実用化、ローカルエアリネットワークの普及等に伴い、かかる通信網を利用して様々な情報をやり取りすることが実現されようとしている。加えて、その情報

2

として動画像データ、静止画像データ、音声データ、コンピュータデータ等のマルチメディア情報を伝送することが考えられている。このような通信網においては、情報を安全に伝達することが重要であり、そのための手段として種々の暗号が知られている。それらの暗号は大きく分けて、共通鍵暗号と公開鍵暗号との２つ暗号方式に分類されるが、それぞれの分類に対して種々の方式が考えられている。

【０００３】図１４は共通鍵暗号通信ネットワーク、図１５は公開鍵暗号通信ネットワークを示す。図１６は共通鍵、公開鍵暗号ネットワークを示し、図１４の共通鍵暗号通信ネットワークに図１５の公開鍵暗号通信ネットワークを付加した構成になっている。

【０００４】まず、共通鍵暗号方式による暗号通信について述べる。共通鍵暗号通信ネットワークでは、図１４に示すように、あらかじめネットワークの加入者間で固有かつ秘密の鍵を共有している。Ａ、Ｂ、Ｃ、…、Ｍはそのネットワークの加入者、K_{AB}、K_{AC}、…はそれぞれ加入者Ａ－Ｂ間で共有している鍵、加入者Ａ－Ｃ間で共有している鍵、…を示している。さらにそれぞれの加入者は、図１７に示すような、ネットワークで決められたアルゴリズムに従って暗号化（及び復号）を行う暗号装置を備えた通信用端末を持っている。従来の加入者ＡからＢへの共通鍵暗号通信は以下の手順で行う。

【０００５】１．Ａは、あらかじめ送信先Ｂと共有している秘密の鍵K_{AB}を本通信の暗号装置の鍵として用いて暗号装置により通信文を暗号化し、その暗号化したものをＢに送信する。

２．Ｂはあらかじめ送信元Ａと共有している秘密の鍵K_{AB}を本通信の暗号装置の鍵として用いて暗号装置によりＡからの受信文を復号し、通信文を得る。

【０００６】次に、公開鍵暗号方式による暗号通信について述べる。図１５に示すように、公開鍵暗号通信ネットワークの電子掲示板には、各加入者の公開鍵が加入者のＩＤ（名前等）と対応がとれる形で掲示されている。図１５においては、加入者Ａ、Ｂ、…、Ｍの公開鍵をK^{p}_{A}、K^{p}_{B}、…、K^{p}_{M}で示している。また各加入者は自分の公開鍵に対応した秘密鍵を秘密に保有する。図１５においては、加入者Ａ、Ｂ、…、Ｍの秘密鍵をK^{s}_{A}、K^{s}_{B}、…、K^{s}_{M}で示している。さらにそれぞれの加入者は、図１７に示されるような、ネットワークで決められたアルゴリズムに従って暗号化（及び復号）を行う暗号装置を備えた通信用端末を持っている。従来の加入者ＡからＢへの公開鍵暗号通信は以下の手順で行う。

【０００７】従来の加入者ＡからＢの公開

１．Ａは送信先Ｂの公開鍵K^{p}_{B}を本通信の暗号装置の鍵として用いて暗号装置により通信文を暗号化し、その暗号化したものをＢに送信する。

２．Ｂは、自分の秘密鍵K^{p}_{B}を本通信の暗号装置の鍵

として用いて暗号装置によりＡからの受信文を復号し、通信文を得る。これらの手順により暗号通信が行われる。

【０００８】以上述べたように、信頼できる通信を実現するために必要な技術である暗号技術に関し、現在のところ知られている代表的な暗号方式に限っても種々の方式が考えられている。また、同じ暗号方式でもいろいろな使用モードが考えられており、さらに暗号解読に対して強度を増すように、いろいろな対策が考えられている。

【０００９】ここで、従来の暗号方式としてＤＥＳ暗号について簡単に説明する。ＤＥＳ暗号では、６４ビットのデータブロックを単位に暗号化及び復号が行われ、鍵の長さは５６ビット（８ビットのパリティビットを加えると６４ビット）とされている。暗号アルゴリズムは転置式と換字式とを基本としており、これらの転置と換字を適当に組み合わせた処理を１６段繰り返すことにより、平文のビットパターンをかき混ぜ、意味の分からない暗号文に変換している。復号する場合は、逆にかき混ぜることにより、元の平文を復元する。

【００１０】このかき混ぜかたのパラメータを５６ビットの鍵で指定する。鍵の候補の数は２の５６乗（約１０の１７乗）個であり、総当たりの解読、つまり入手した暗号文と平文のペアに対し、鍵を１回ずつ変化させてチェックする解読を行うと、１回のチェックに５００ｎｓかかるとすると（１２８Ｍｂｐｓの処理速度）、全体で１０００年程度かかる計算になる。

【００１１】ＤＥＳの暗号化処理では、まず６４ビットの平文に対して転置（初期転置ＩＰ）が行われる。この初期転置は固定である。この転置処理の出力は途中複雑な１６段の暗号化処理を経た後に最後に転置（最終転置IP^{-1}）が行われる。この最終転置も固定である。

【００１２】初期転置が行われた６４ビットのデータは、３２ビットずつ左右に分割され左半分がL_0、右半分がR_0となる。このL_0とR_0からL_{16}とR_{16}になるまで１６段にわたって図１８に示す処理が行われる。つまり、ｎ段目の処理を終了したときの左右の３２ビットをそれぞれL_0、R_0とすると、L_n、R_nは次式で表されるものとなる。

【００１３】$L_n = R_{n-1}$

$R_n = L_{n-1} \# f(R_{n-1}, K_n)$

【００１４】ここで、＃はビット毎のｍｏｄ２の排他的論理和を意味し、K_nはｎ段目に入力される４８ビットの鍵、L_{n-1}とR_{n-1}はそれぞれｎ－１段目の出力、ｆはR_{n-1}とK_nを用いて３２ビットのデータを出力する関数である。

【００１５】

【発明が解決しようとする課題】しかしながら、従来の暗号通信においては、送信側と受信側でどの暗号方式や使用モードを使用し、また暗号解読に対してどのような

対策を施した方式を使用して暗号通信を行うのかという調整に関しては考慮されていなかった。そのため、送信者と受信者で複数の暗号方式を実行できる暗号装置を持つ場合や、複数の使用モードが実行できる場合に、どのようにして送受信者間で調整を行うことにより、暗号通信を行うのか、あるいは両者の共通の暗号方式を検知して、その暗号方式により暗号通信を行う、というようなことができなかった。

【００１６】さらに、やり取りする情報の種類に応じて、送信側と受信側とで暗号方式を打ち合わせるなどの調整に関しては考慮されていなかった。特に、やり取りする情報の種類に応じて暗号の強度を調整することに関しては考慮されてなかった。例えば、やり取りする情報が機密性の高い情報であれば従来の技術で述べたような暗号解読に対し対策を施した方式を用いて安全性の高い暗号通信を行い、やり取りする情報が機密性の高い情報でなければ、通常の暗号方式を用いることにより、暗号装置の負荷を軽減する、というようなことができなかった。従来の暗号通信においては、以上のような問題があった。

【００１７】本発明は、上記の問題点を解決するために成されたもので、暗号方式を選択できる暗号通信装置、システム及び暗号装置を得ることを目的としている。

【００１８】

【課題を解決するための手段】請求項１の発明においては、それぞれ送信データの暗号化及び受信暗号化データの復号を行い、互いに通信を行う複数の通信手段と、上記通信手段に設けられ、複数の暗号化方式の１つを選択する選択手段とを設けている。

【００１９】請求項７の発明においては、複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、動作モードを指定するモード指定手段とを備え、上記暗号化手段は、指定されたモードに応じて暗号化方式を選択する。

【００２０】請求項８の発明においては、複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、セキュリティランクを指定する指定手段とを備え、上記暗号化手段は、指定されたセキュリティランクに応じて暗号化方式を選択する。

【００２１】請求項９の発明においては、ネットワーク上の複数端末間で暗号化されたデータの通信を行うとともに、暗号化方式を選択し得るようにした暗号通信システムであって、所定の端末装置により指定された暗号化方式を他の端末装置により変更する場合に、上記所定の端末装置側の承諾を必要とする。

【００２２】

【作用】本発明によれば、暗号通信を行う送受信者の利用する通信手段に、暗号方式を選択できる選択手段を設けることにより、暗号方式を任意に設定できると共に、その設定した暗号方式を暗号文の送信に先立って送受信

5

者間で共有することにより、従来考慮されていなかった暗号方式の選択を可能にし、自由度の高い暗号通信を可能にしている。また、暗号強度の選択も可能にしている。

【００２３】

【実施例】以下に実施例１～８を示すが、各実施例は次に示すような観点から成り立っている。

［実施例１］　複数の暗号の中から暗号方式を設定する。

［実施例２］　共通鍵暗号と公開鍵暗号の中から暗号方式を設定する。

［実施例３］　複数のブロック暗号の中から暗号方式を設定する。

［実施例４］　ＤＥＳ型暗号に対し、複数のｆ関数を用意し、それらを選択することにより、暗号方式を設定する。

【００２４】［実施例５］　ブロック暗号に対し、使用モードの中から暗号方式を設定する。

［実施例６］　「鍵を更新しながら暗号化を行う」複数の暗号方式の中から暗号方式を設定する。

［実施例７］　ブロック暗号に対し、「固定の鍵を用いて暗号化を行う」暗号方式と、「鍵を更新しながら暗号化を行う」暗号方式の中から暗号方式を設定する。

［実施例８］　実施例７の「鍵を更新しながら暗号化を行う」暗号方式の鍵生成・選択装置の内部変数を読み出し可能にする。

【００２５】ただし、本発明の本質は、複数の暗号方式の中から特定の暗号方式を実行できるように選択する手段を有することにある。また、それによって暗号の強度を選択できるようにしたことにある。従って、選択される複数の暗号方式としては、実施例に示した暗号方式に限定されるものではない。従来の技術でも述べたが、現在提案されている暗号方式は多数存在するため、その全ての暗号方式について実施例で示すことは困難である。また、複数の暗号方式を組み合わせたような暗号方式も、本発明により選択される暗号方式として含まれる。

【００２６】［実施例１］本実施例では、図１に示すように、暗号化（及び復号）を行う複数の暗号装置１１と、通信インタフエース１２と、鍵生成・選択装置１３と、複数の暗号装置１１の出力の中から１つを選択する選択手段１４とを備えた通信用端末１０を用いて暗号通*

$$x_{i+1} = f(x_i) \quad (i = 0, 1, \cdots) \qquad \cdots\cdots\cdots (1)$$

$$b_{i+1} = g(x_{i+1}) \quad (i = 0, 1, \cdots) \qquad \cdots\cdots\cdots (2)$$

【００３２】鍵生成・選択装置１３は、図２に示すように、式（１）のフィードバック演算を行う処理回路１３ａと、式（２）の演算を行う処理回路１３ｂと、暗号方式設定信号で選択された暗号方式に対応した鍵に必要な長さの出力が、式（２）の演算を行う処理回路１３ｂから出されたときにそれを鍵に変換する演算器１３ｃとから構成される。

6

*信を行う。

【００２７】各々の暗号装置１１は、それぞれ異なる暗号方式の処理を実現する。本実施例では暗号方式として、

・暗号方式１
・暗号方式２
・…
・暗号方式ｔ

のｔ種類の暗号とし、それぞれ暗号装置１、暗号装置２、…、暗号装置ｔの各暗号装置１１でその処理が実現されているとする。さらに、どの暗号装置１１を使用するかを暗号方式設定信号により設定できる。尚、以下の説明では、暗号装置１１を必要に応じて暗号装置１…ｔと呼ぶものとする。

【００２８】選択手段１４は、暗号方式設定信号によって制御され、複数の暗号装置１１の出力の中から１つ選択することができる。例えば、暗号方式１の暗号処理を行いたい場合には、暗号方式設定信号によって選択手段１４を暗号装置１からの出力を選択するように設定すればよい。同様に暗号方式２の暗号処理を行いたい場合には暗号方式設定信号によって選択手段１４を暗号装置２からの出力を選択するように設定すればよい。

【００２９】通信インタフェース１２は、暗号方式を示す情報と暗号装置１１で暗号化された送信文とを伝送路に送信するとともに、通信相手からの暗号方式を示す情報と暗号装置１１で暗号化された送信文とを伝送路から受信するための通信インタフェースである。

【００３０】さらに、一般に暗号方式毎に鍵の長さは異なっているため、暗号方式設定信号によって選択された暗号方式に対応した鍵を生成、または選択する手段として鍵生成・選択装置１３がある、鍵生成・選択装置１３では、ある長さを持つ１つの鍵から選択された暗号方式に対応した鍵を生成する。あるいはあらかじめ暗号装置で実現できる暗号方式の数だけ対応する鍵を用意しておき、選択された暗号方式に対応した鍵を選択する。

【００３１】図２に本発明による鍵生成・選択装置１３の一例を示す。鍵生成・選択装置１３は、次に示すようなアルゴリズムに従って鍵を生成する。鍵生成・選択装置１３に入力されるある長さを持つ１つの鍵は、以下のアルゴリズムで初期値（x_0）として用いられる。

【００３３】演算器１３ｃでは、式（２）の演算を行う処理回路１３ｂから出力されるb_1、b_2、…、b_lを暗号方式設定信号で選択された暗号方式に対応した長さの鍵に変換することを行う。鍵は選択された暗号方式のアルゴリズムで定められた長さのビット列であり、演算器１３ｃによって例えばb_1、b_2、…、b_lをそのまま並べることにより、あるいはその順序を並び変えるこ

とにより生成される。

【００３４】従って、鍵生成・選択装置１３の動作は以下のようになる。

１．初期値としてx_0を、鍵生成・選択装置１３に入力する。

２．式（１）により、x_1、x_2、…、x_tを生成する。

３．生成されたx_1、x_2、…、x_tに対して式（２）を実行し、得られたb_1、b_2、…、b_tを出力する。

４．演算器１３ｃによりb_1、b_2、…、b_tを暗号方式設定信号で選択された暗号方式に対応した鍵として出力する。

【００３５】鍵生成・選択装置１３は、暗号方式設定信号によって、式（１）及び式（２）の演算を何回行うか、さらに演算器１３ｃからどれだけの長さの鍵を出力するか、を制御され、そのことにより暗号方式設定信号によって選択された暗号方式に対応した長さを持つ鍵を生成する。

【００３６】また、鍵生成・選択装置１３は図３のように構成することも可能である。図３の鍵生成・選択装置１３はｔ個の鍵（k_1、k_2、…、k_t）と鍵選択手段１３ｄとから構成される。鍵k_1、k_2、…、k_tは鍵選択手段１３ｄに入力され、暗号方式設定信号によっていずれかが選択される。これにより暗号方式設定信号によって選択された暗号方式に対応した長さを持つ鍵を選択する。

【００３７】上記通信用端末１０を用いて暗号通信を行う暗号通信ネットワークとしては図１４のものを用いる。鍵の共有は、あらかじめネットワークの管理者等が鍵の設定しておくことによって実現できる。あるいは、文献「暗号と情報セキリュティ」（辻井、笠原著、１９９０年発行、株式会社昭晃社、７２～７３、９７～１０４項）示されるような公知の鍵共有方式によっても実現できる。

【００３８】本発明による加入者ＡからＢへの暗号通信は以下の手順で行われる。以下の説明では、鍵生成・選択装置１３としては、図２に示すものであるとし、上記のように、ある長さを持つ１つの鍵から選択された暗号方式に対応した鍵を生成する。

【００３９】［本発明による暗号通信の前手順１］

１．送信者Ａは、暗号方式を示す情報を通信インタフェース１２を介して受信者Ｂに送る。

２．受信者Ｂは、送信者Ａから送られてきた暗号方式を示す情報を情報通信インタフェース１２を介して受信し、受信者Ｂが利用している通信用端末１０にある暗号装置１１がその暗号方式で処理できることを確認し、暗号通信の開始の了解を通信インタフェース１２を介して送信者Ａに伝える。その暗号方式で処理することが困難な場合には、可能な暗号方式を通信インタフェース１２を介して送信者Ａに伝える。

３．上記手順を送受信者間で暗号方式に関して合意ができるまで繰り返す。

【００４０】上記の前手順１では、暗号方式を示す情報を送信者の方から示したが、逆に次のように受信者の方から示すことも可能である。

［本発明による暗号通信の前手順２］

１．受信者Ｂは、情報の提供の要求とその情報を暗号化する時の暗号方式を示す情報を通信インタフェース１２を介して送信者Ａに送る。

２．送信者Ａは、受信者Ｂから送られてきた情報の提供の要求と暗号方式を示す情報とを情報通信インタフェース１２を介して受信し、送信者Ａが利用している通信用端末１０にある暗号装置がその暗号方式で処理できることを確認し、暗号通信の開始の了解を通信インタフェース１２を介して受信者Ｂに伝える。その暗号方式で処理することが困難な場合には、可能な暗号方式を通信インタフェース１２を介して受信者Ｂに伝える。

３．上記手順を送受信者間で暗号方式に関して合意ができるまで繰り返す。

【００４１】上の手順は送信者が受信側の設定可能な暗号方式を知らない場合、あるいは受信者が送信側の設定可能な暗号方式を知らない場合に有効な手順である。送信者が受信側で設定可能な暗号方式を知っている場合、又は受信者が送信側の設定可能な暗号方式を知っている場合には、上記の手順１、だけを行って次の暗号通信を開始することが可能である。

【００４２】さらに、暗号通信に先立って暗号鍵を送受信者間で交換するような鍵共有方式を行うような暗号通信ネットワークにおいては、鍵共有のプロトコルにおいて、鍵の共有のための情報と共に暗号方式の情報も共有することが可能である。そのような場合には、上記の手順を省略して暗号通信を開始することが可能である。

【００４３】上記前手順１、２によれば、送受信者間で暗号方式を調整することができる。また、上記前手順１、２は通信毎に毎回行う必要はない。例えば、あらかじめ暗号方式を送受信者間で打ち合わせておき、その暗号方式で暗号通信を行う場合には必要ない。

【００４４】以下、送信者Ａと受信者Ｂとの間で次の手順を続ける。

［本発明によるデータの暗号通信手順（送信者Ａに関する）］

１．暗号方式設定信号により、前手順１、２で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ受信者Ｂと共有している秘密の鍵K_{AB}を通信用端末１０内の鍵生成・選択装置１３に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵を生成する。生成された鍵は暗号装置１１に設定される。

３．暗号装置１１によりデータを暗号化し、選択手段１

４により前手順で決定した暗号装置１１から出力される暗号文を選択し、通信インタフェース１２を介してＢに送信する。

【００４５】［本発明によるデータの暗号通信手順（受信者Ｂに関する）］

１．暗号方式設定信号により、前手順１、２で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ送信者Ａと共有している秘密の鍵K_{AB}を通信用端末１０内の鍵生成・選択装置１４に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵を生成する。生成された鍵は暗号装置１１に設定される。

３．通信インタフェース１２を介して伝送路から暗号化データを受信し、暗号装置１１によりＡから送られてきた暗号化データを復号し、選択手段１４により前手順で決定した暗号装置１１から出力される平文を選択する。

【００４６】また、鍵生成・選択装置１３として図３のものを用いることも可能である。その場合には、図１４に示された鍵は、複数の鍵を合わせたものを意味する。つまり、加入者ＡとＢの間の鍵K_{AB}は、暗号方式１を使う時の鍵K_{AB1}、暗号方式２を使う時の鍵K_{AB2}、…、暗号方式ｔを使う時の鍵K_{ABt}からなる。この場合の本発明による加入者ＡからＢへの暗号通信は以下の手順で行われる。ただし、前手順１、２は上記と同じなので省略する。

【００４７】［本発明によるデータの暗号通信手順（送信者Ａに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ受信者Ｂと共有している秘密の鍵K_{AB}（K_{AB1}、K_{AB2}、…、K_{ABt}から構成される）を通信用端末１０内の鍵生成・選択装置１３に設定し、暗号方式設定信号により、複数の鍵K_{AB1}、K_{AB2}、…、K_{ABt}から選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１１に設定される。

３．暗号装置１１によりデータを暗号化し、選択手段１４により前手順で決定した暗号装置１１から出力される暗号文を選択し、通信インタフェース１２を介してＢに送信する。

【００４８】［本発明によるデータの暗号通信手順（受信者Ｂに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ送信者Ａと共有している秘密の鍵K_{AB}（K_{AB1}、K_{AB2}、…、K_{ABt}から構成される）を通信用端末１０内の鍵生成・選択装置１３に設定し、暗号方式設定信号により、複数の鍵K_{AB1}、K_{AB2}、…、K_{ABt}から選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１１に設定される。

３．通信インタフェース１２を介して伝送路から暗号化データを受信し、暗号装置１１によりＡから送られてきた暗号化データを復号し、選択手段１４により前手順で決定した暗号装置１１から出力される平文を選択する。

【００４９】また暗号通信ネットワークの加入者はそれぞれ、暗号通信するために必要な各ユーザの鍵などの秘密情報を格納するために、図４に示されるような携帯型記憶装置３０を保有していてもよい。携帯型記憶装置３０には、暗号通信するために必要な各ユーザの秘密情報が格納されており、安全性を考慮して通信用端末１０とは別に各ユーザ毎に携帯型記憶装置３０を持つような構成にしている。各ユーザ毎に物理的に安全な領域が確保できるなら携帯型記憶装置３０は通信用端末１０の一部であってもよいが、その場合は各ユーザ毎に暗号通信に使用できる通信用端末１０が制限されてしまう。通信用端末１０と携帯型記憶装置３０とを分離し、通信用端末１０には各ユーザの秘密情報を格納しないようにすることで、ユーザはどの通信用端末１０でも自分の携帯型記憶装置３０を介してそのユーザの秘密情報をやりとりして暗号通信に使用することが可能となり便利である。

【００５０】携帯型記憶装置３０は、上記通信用端末と安全な通信路を介して情報のやり取りを行えるようになっており、物理的に安全な領域を保持手段３０ａとして持つ。携帯型記憶装置３０を正常に動作させることができるのは正規の所有者だけであり、パスワード等の認証手続きにより正規の所有者か否かを判断する。また、上記の共有鍵のうちその携帯型記憶装置３０の所有者に関係するものを保持手段３０ａに保持している。携帯型記憶装置３０はＩＣカード等により実現できる。以下に説明する全ての実施例２～８において、この携帯型記憶装置３０を用いる場合に関しても本発明の範囲である。

【００５１】［実施例２］本実施例では、図５に示すような、暗号化（及び復号）を行う複数の暗号装置１５、１６と、通信インタフエース１２と、鍵生成・選択装置１３と、複数の暗号装置１５、１６の出力の中から１つを選択する選択手段１４とを備えた通信用端末１０を用いて暗号通信を行う。

【００５２】本実施例では、暗号方式を

１．共通鍵暗号方式の代表としてＤＥＳ暗号方式（またはＦＥＡＬ暗号方式）

２．公開鍵暗号方式の代表としてＲＳＡ暗号方式（またはＥｌＧａｍａｌ暗号方式）の２種類の暗号方式とし、それぞれＤＥＳ暗号装置（またはＦＥＡＬ暗号装置）１５と、ＲＳＡ暗号装置（またはＥｌＧａｍａｌ暗号装置）１６とでその処理が実現されているものとする。ただし、ここで例示したＤＥＳ暗号、ＦＥＡＬ暗号、ＲＳＡ暗号、ＥｌＧａｍａｌ暗号は、共通鍵暗号或は公開鍵暗号の代表例として挙げただけで、本発明はこれらに限

定されず他の暗号アルゴリズムにも適用可能である。

【００５３】図５の通信用端末１０をＤＥＳ暗号方式で使用する場合には、選択手段１４ではＤＥＳ暗号装置１５からの出力を選択するようにすればよい。図５の通信用端末１０をＲＳＡ暗号方式で使用する場合には、選択手段１４ではＲＳＡ暗号装置１６からの出力を選択するようにすればよい。

【００５４】鍵生成・選択装置１３、通信インタフェース１２、選択手段１４は、実施例１と同様のものを用いる。ただし、鍵生成・選択装置１３は図３に示されたものを用い、暗号方式設定信号によって選ばれた暗号方式に対応する鍵を選択する。つまり、ＤＥＳ暗号方式が選ばれた場合は、ＤＥＳ暗号用にあらかじめ配布されている鍵を選択し、ＲＳＡ暗号方式が選ばれた場合は、ＲＳＡ暗号用に公開されている公開鍵を選択する。

【００５５】また、本実施例では、暗号通信ネットワークとしては図１６のものを用いる。図１６の共通鍵、公開鍵暗号通信ネットワークは図１４の共通鍵暗号通信ネットワークに図１５の公開鍵暗号通信ネットワーク付加した構成になっている。

【００５６】本発明による加入者ＡからＢへの暗号通信は、以下の手順で行われる。ただし、前手順１、２は実施例１と同様である。

［本発明によるデータの暗号通信手順（送信者Ａに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．暗号方式設定信号により、共通鍵K_{AB}と公開鍵K^{P}_{B}とから選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１５、１６に設定される。

３．暗号装置１５、１６によりデータを暗号化し、選択手段１４により前手順で決定した暗号装置から出力される暗号文を選択し、通信インタフェース１２を介してＢに送信する。

【００５７】［本発明によるデータの暗号通信手順（受信者Ｂに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．暗号方式設定信号により、共通鍵K_{AB}と公開鍵K^{S}_{B}とから選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置１５、１６に設定される。

３．通信インタフェース１２を介して伝送路から暗号化データを受信し、暗号装置によりＡから送られてきた暗号化データを復号し、選択手段１４により前手順で決定した暗号装置から出力される平文を選択する。

【００５８】この手順により、送受信者間で暗号方式について調整することができ、暗号通信の安全性を選択することができる。つまり、送信するデータの機密性に応じて暗号方式を選択できる。例えば，特に機密性の高いデータの場合には、公開鍵暗号方式を選択し、そうでない場合には、共通鍵暗号方式を選択して処理を簡易にする。というようなことができる。

【００５９】［実施例３］本実施例では、図６に示されるような、暗号化（及び復号）を行う複数の暗号装置１７、１８と、通信インタフエース１２と、鍵生成・選択装置１３と、複数の暗号装置１７、１８の出力の中から１つを選択する選択手段１４とを備えた通信用端末１０を用いて暗号通信を行う。

【００６０】本実施例では、暗号方式として

１．ＤＥＳ暗号

２．ＦＥＡＬ暗号

の２種類のブロック暗号とし、それぞれＤＥＳ暗号装置１７と、ＦＥＡＬ暗号装置１８とでその処理が実現されるものとする。ただし、ここで例示したＤＥＳ暗号、ＦＥＡＬ暗号は共通鍵暗号の代表例として挙げただけで、本発明はこれらに限定されず他の暗号アルゴリズムも適用可能である。

【００６１】図６の通信用端末１０を用いてＤＥＳ暗号処理を行いたい場合は、選択手段１４では常にＤＥＳ暗号装置１７からの出力を選択するようにすればよい。また、ＦＥＡＬ暗号処理を行いたい場合は、選択手段１４では常にＦＥＡＬ暗号装置１８からの出力を選択するようにすればよい。

【００６２】鍵生成・選択装置１３、通信インタフェース１２、選択手段１４は、実施例１と同様のものを用いる。また、上記通信用端末１０を用いて暗号通信を行う暗号通信ネットワークとしては図１４のものを用いる。そして本実施例による加入者ＡからＢへの暗号通信は実施例１と同様の手順で行われる。

【００６３】［実施例４］本実施例では、図７に示すような、暗号化（及び復号）を行う暗号装置１９と、通信インタフエース１２と、鍵生成・選択装置１３とを備えた通信用端末１０を用いて暗号通信を行う。また、これまでの実施例１～３で用いている選択手段１４は、本実施例では暗号装置１９内に含まれている。

【００６４】本実施例では、暗号方式としてＤＥＳ型（インボリューション型）暗号を用いる。その構成要素であるｆ関数を複数用意し、その中からあるｆ関数を選択することにより、複数の暗号方式を設定できる。ＤＥＳ型暗号は前述したように同じ処理を繰り返すアルゴリズムであるので、同じ回路で繰り返し処理を行うことが可能である。例えば図１８に示されたＤＥＳ暗号の１段分の１処理単位として回路化すれば、その回路を繰り返し用いることにより、暗号処理を実現できる。

【００６５】この場合の暗号装置１９は図８のように構成される。図８の暗号装置１９は、レジスタ１９ａ、１９ｂと、排他的論理和回路１９ｃと、複数のｆ関数（f_1、f_2、…、f_t）と、複数のｆ関数の出力から１つ

を選択する選択手段１９ｄとから構成される。選択手段１９ｄは、暗号方式設定信号によって制御されている。

【００６６】複数のｆ関数の構成は、例えばｆ関数と同じ数のＳｂｏｘの組を用意しておくことにより実現可能である。この場合には、ｆ関数f_1に対してはS_{11}、S_{12}、…、S_{18}のＳｂｏｘを用い、ｆ関数f_2に対してはS_{21}、S_{22}、…、S_{28}のＳｂｏｘを用い、…、というようにすればよい。また、ｆ関数f_1に対してはＤＥＳ暗号のｆ関数を用い、ｆ関数f_2に対してはＦＥＡＬ暗号のｆ関数を用い、…、というように、全く異なる暗号のｆ関数を用意することによっても実現できる。

【００６７】以上説明したような暗号装置１９を用いて、実施例１と同様の手順により暗号通信を行うことが可能である。尚、鍵生成・選択装置１３、通信インタフェース１２は、実施例１と同様のものを用いる。本実施例でも、暗号通信ネットワークとしては図１４のものを用いる。本実施例により、送受信者間で暗号方式について調整することができる。

【００６８】［実施例５］本実施例では、図７に示す通＊信用端末１０と同一構成の通信用端末を用いて暗号通信を行う。ただし、図７の暗号装置１９に代えて図９に示すような暗号装置２０を用いる。また、選択手段は本実施例でも暗号装置２０内に含まれている。また、本実施例では、暗号方式によって鍵のビット長は変わらないので鍵生成・選択装置１３は必ずしも必要ではない。

【００６９】本実施例では、暗号方式としてブロック暗号を考える。さらに、そのブロック暗号を

１．ＥＣＢ（Ｅｌｅｃｔｒｉｃ　Ｃｏｄｅｂｏｏｋ）モード

２．ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モード

のどちらで使用するか暗号方式設定信号により設定できるものとする。

【００７０】ＣＢＣモードについては後述するが、ここでも簡単に説明しておく。平文をM_i、暗号文をC_i、初期値をＩＶとし、暗号鍵Ｋを用いた暗号化をE_k、復号をD_kとするとＣＢＣモードは次式で表される。

$$C_1 = E_k(M_1 + IV) \quad \cdots\cdots (3)$$

$$C_i = E_k(M_i + C_{i-1}) \quad (i = 2, 3, \cdots) \quad \cdots\cdots (4)$$

$$M_1 = D_k(C_1) + IV \quad \cdots\cdots (5)$$

$$M_i = D_k(C_i) + C_{i-1} \quad (i = 2, 3, \cdots) \quad \cdots\cdots (6)$$

【００７１】この場合の暗号装置２０は図９のように構成される。図９の暗号装置２０は、ブロック暗号器２０ａと、２つの入力から一方を選択する選択手段２０ｂと、ビット毎に排他的論理和演算を行う排他的論理和回路２０ｃとからなる。選択手段２０ｂは、暗号方式設定信号によって制御されている。

【００７２】この暗号装置２０をＥＣＢモードで使用する場合には、入力する初期値ＩＶとして全て０のビット列とし、選択手段２０ｂでは常に初期値ＩＶを選択するようにすればよい。また暗号装置２０をＣＢＣモードで使用する場合には、入力する初期値ＩＶとして任意のビット列を設定し、選択手段２０ｂでは初期のブロックを暗号化する時には初期値ＩＶを選択するようにし、以降は暗号装置２０からの出力を選択するようにすればよい。初期値ＩＶは通信者間で秘密にする必要はない。

【００７３】以上説明したような暗号装置２０を用いて、実施例１と同様の手順により暗号通信を行うことが可能である。ただし、前手順において、ＣＢＣモードを選択した場合には、初期値ＩＶを共有する手順が必要となる。例えば、暗号通信を行う前にＡからＢへ初期値ＩＶを送信する手順が必要となる。初期値ＩＶは送受信者間で秘密にする必要はないので、暗号化しなくてもよい。また、秘密の鍵K_{AB}だけでなく、共有した初期値ＩＶを通信用端末１０内の暗号装置２０に設定しなければならない。

【００７４】鍵生成・選択装置１３通信インタフェース１２は実施例１と同じものを用いる。本実施例でも、暗号通信ネットワークとしては図１４のものを用いる。本実施例により、送受信者間で暗号方式の使用モードを調整することができる。

【００７５】［実施例６］本実施例は、実施例１に基づいて暗号方式を改良したものである。本実施例では、実施例１と同じく、図１に示す通信用端末１０を用いて暗号通信を行う。

【００７６】本実施例が実施例１と異なる点は以下の通りである。実施例１では暗号装置１１は複数存在したが、各々の暗号装置１１に対する鍵は一度の暗号通信を行っている間は固定である。つまり、暗号通信中には鍵が随時変更されるということはなく、暗号通信の初めから終わりまで同一の鍵を用いる。それに対して本実施例では、第３者による暗号解読に対して安全性を向上させるために、暗号通信中に鍵を随時変更する。暗号通信中に鍵を随時更新するために、鍵生成・選択装置１３では暗号通信中も鍵生成を行い、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成される毎に、暗号装置１１の鍵の更新を行う。ただし、鍵の更新は暗号通信の送信者と受信者とで同期をとって行う必要がある。

【００７７】本実施例の鍵生成・選択装置１３も、実施例１の場合と同じく図２のように構成される。ただし、本実施例の鍵生成・選択装置１３では上述のように、暗号通信中も鍵生成を行い、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成される毎に、暗号装置１１の鍵の更新をする、ということを行うため、実

施例１の場合と動作が異っている。

【００７８】実施例１の場合の鍵生成・選択装置１３は、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成されればそれ以上動作させる必要はない。それに対して本実施例での鍵生成・選択装置１３では、暗号方式設定信号で選択された暗号方式に対応した長さの鍵を次々に生成する必要がある。つまり、本実施例での鍵生成・選択装置１３は、実施例１の場合の鍵生成・選択装置１３の動作を何度も繰り返し行っている。

【００７９】本発明に用いる鍵生成・選択装置１３の鍵生成のアルゴリズムは、特に制限を受ける訳ではなく、＊

$$x_{i+1} = x_i^2 \bmod N \quad (i = 0, 1, 2, \cdots) \qquad \cdots\cdots\cdots (7)$$

$$b_i = lsb_j(x_i) \quad (i = 1, 2, \cdots) \qquad \cdots\cdots\cdots (8)$$

によって得られるビット系列b_1、b_2、…を２乗型疑似乱数系列という。但し、$lsb_j(x_i)$はx_iの下位ｊビットを表わし、Ｎのビット数をｎとしたときｊ＝Ｏ（$\log_2 n$）とする。

【００８１】２乗疑似乱数系列は、法Ｎにおける平方剰余性の判定問題が計算量的に困難であるとの仮定の下で計算量的に安全な疑似乱数系列となる。２乗疑似乱数を十分安全なものとするため、２乗演算式（７）の法Ｎのビット数ｎを５１２ビット程度とすることが望ましい。さらに、各加入者間であらかじめ秘密に共有されている鍵（鍵生成・選択装置の初期値）K_{AB}、K_{AC}、…は、１＜K_{AB}、K_{AC}、…＜Ｎ－１とする。

【００８２】この２乗疑似乱数系列を用いた鍵生成・選択装置１３は図１０に示される。図１０の鍵生成・選択装置１３は式（７）のフィードバック演算を行う処理回路１３ｅと式（８）の演算を行う処理回路１３ｆと演算装置１３ｇとから構成される。この鍵生成・選択装置１３の動作は以下のようになる。

１．初期値x_0を鍵生成・選択装置１３に入力する。

２．式（７）により、x_1、x_2、…を生成する。

３．生成されたx_1、x_2、…に対し、式（８）を実行し、得られたb_1、b_2、…を出力する。

４．演算器１３ｇではb_1、b_2、…を暗号方式設定信号で選択された暗号方式に対応した長さの鍵の鍵列k_1、k_2、…に変換する。

【００８３】図１１に鍵を随時更新する場合の暗号通信の図を示す。暗号方式としてブロック暗号を考える。図１１において、M_{uv}（ｕ＝１、２、…、ｔ；ｖ＝１、２、…、ｓ）は平文ブロックを、k_u（ｕ＝１、２、…、ｔ）はブロック暗号の鍵を、$k_u(M_{uv})$（ｕ＝１、２、…、ｔ；ｖ＝１、２、…、ｓ）は平文ブロックM_{uv}を鍵k_uで暗号化して得られる暗号文ブロックを示している。ここで、M_{u1}からM_{us}までのｓ個のブロックは同じ鍵k_uで暗号化されている。前述の鍵生成・選択装置１３によって更新される鍵系列k_1、k_2、…を順にブロック暗号の鍵として用いることにより、図１１の平文ブロックは複数の暗号鍵によって暗号化される。これのように随時鍵を更新することにより、同じ鍵で暗号化される平文ブロックの数がｓ個になり、鍵の解析を困難にすることができる。尚、本実施例でも、暗号通信ネットワークとしては図１４のものを用いる。

＊実施例１で示したような一般的なものを用いることが可能であるが、本実施例では鍵生成のアルゴリズムとして、計算量的に安全な疑似乱数系列生成アルゴリズムを用いた場合、特にその中でも２乗型疑似乱数系列を用いた場合について説明する。

【００８０】２乗型疑似乱数系列とは、以下の手順で生成される疑似乱数系列b_1、b_2、…である。

［２乗型疑似乱数系列］ｐ、ｑをｐ≡ｑ≡３（ｍｏｄ４）である素数とし、Ｎ＝ｐ・ｑとして、初期値x_0（１＜x_0＜Ｎ－１なる整数）と再帰式

【００８４】加入者ＡからＢへの暗号通信は、以下の手順で行われる。ただし、前手順は実施例１と同様である。

［本発明によるデータの暗号通信手順（送信者Ａに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ受信者Ｂと共有している秘密の鍵K_{AB}を通信用端末１０内の鍵生成・選択装置１３に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵列を生成する。

３．鍵生成・選択装置１３から出力される鍵列を暗号装置１１の鍵として随時更新しつつ用いデータを暗号化し、選択手段１４により前手順で決定した暗号装置１１から出力される暗号文を選択し、通信インタフェース１２を介してＢに送信する。

【００８５】［本発明によるデータの暗号通信手順（受信者Ｂに関する）］

１．暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段１４を設定する。

２．あらかじめ送信者Ａと共有している秘密の鍵K_{AB}を通信用端末１０内の鍵生成・選択装置１３に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵列を生成する。

３．通信インタフェース１２を介して伝送路から暗号化データを受信し、鍵生成・選択装置１３から出力される鍵列を暗号装置１１の鍵として随時更新しつつ用いて、送られてきた暗号化データを復号し、選択手段１４により前手順で決定した暗号装置１１から出力される平文を選択する。

【００８６】また、計算量的に安全な疑似乱数生成のア

ルゴリズムとして２乗型疑似乱数を用いたが、計算量的に安全な疑似乱数生成アルゴリズムであればどのようなものでも用いることができる。たとえば前記文献「暗号と情報セキュリティ」（辻井、笠原著、１９９０年発行、株式会社昭晃社、８６頁）に示されているように、ＲＳＡ暗号、離散対数、逆数暗号を用いたものも本発明の疑似乱数生成のアルゴリズムに用いることができる。また、本実施例で説明した鍵を随時更新する方法は、実施例１に基づいて説明したが、実施例１に適用できるだけでなく、実施例３、４、５に対しても適用できる。

【００８７】［実施例７］実施例１は鍵は固定の暗号方式（複数）の中からある暗号方式を選択し、実施例６は鍵は更新される暗号方式（複数）の中からある暗号方式を選択するものである。上記２つの実施例１、６のバリエーションとして本実施例では、鍵は固定の暗号方式と鍵は更新される暗号方式との間で暗号方式を選択できるようにしている。また、本実施例では、図１２に示されるような、暗号化（及び復号）を行う暗号装置１１と、通信インタフェース１２と、鍵生成・選択装置１３を備えた通信用端末１０を用いて暗号通信を行う。ここでは、説明の簡単のため暗号装置１１は１つであるとする。

【００８８】本実施例では、暗号方式としてブロック暗号を考える。さらに、そのブロック暗号を、

１．固定の鍵を用いて暗号化を行う。

２．鍵を更新しながら暗号化を行う。

のどちらの方式を使用するか暗号方式設定信号により設定できるものとする。

【００８９】鍵生成・選択装置１３は暗号方式設定信号によって制御され、「固定の鍵を用いて暗号化を行う」暗号方式で使用する場合には、鍵生成・選択装置１３は固定鍵（１つの鍵）を生成すれば処理を停止する。また、鍵を更新しながら暗号化を行う」暗号方式で使用する場合には、鍵生成・選択装置１３は鍵列（複数の鍵）を生成するために処理を繰り返し行う、という動作を行う。図１２の通信用端末１０を「固定の鍵を用いて暗号化を行う」暗号方式で使用する場合には、暗号方式設定信号により鍵生成・選択装置１３では固定鍵を生成するようにし、暗号装置１１ではその固定鍵を用いて暗号化すればよい。また、図１２の通信用端末１０を「鍵を更新しながら暗号化を行う」暗号方式で使用する場合には、暗号方式設定信号により鍵生成・選択装置１３では鍵列を生成するようにし、暗号装置１１ではその鍵列により順次鍵を更新しながら暗号化すればよい。鍵生成・選択装置１３は図２と同じ構成で動作が実施例６と同じものを用いる。暗号装置１１、通信インタフェース１２は実施例１と同じものを用いる。また、暗号通信ネットワークとしては図１４のものを用いる。

【００９０】加入者ＡからＢへの暗号通信は、実施例１と同様の手順で行われる。ただし、鍵を更新しながら暗号化を行うことを選択した場合には、データの暗号通信手順は実施例６と同様の手順で行われる。

【００９１】本実施例により、送受信者間で暗号方式について調整することができ、暗号通信の安全性を選択することができる。つまり、送信するデータの機密性に応じて暗号方式を選択できる。例えば、特に機密性の高いデータの場合には、「鍵を更新しながら暗号化を行う」暗号方式を選択し、そうでない場合には、「固定の鍵を用いて暗号化を行う」暗号方式を選択して処理を簡易にする、というようなことができる。尚、本実施例では説明の簡単のため、暗号装置１１は１つとしたが、複数の暗号装置１１を用いてもよい。その場合には、複数の暗号装置１１からの出力を選択するための選択手段１４が必要となる。

【００９２】［実施例８］本実施例は、実施例６、７で用いた鍵生成・選択装置１３の構成を少し変えた場合である。実施例６、７では、各加入者間で共有されている鍵が固定のため、「鍵を更新しながら暗号化を行う」暗号方式においても、送受信者が同じ場合には鍵生成・選択装置１３の初期値は常に同じ値となり、同じ鍵列が生成されるという問題がある。

【００９３】そこで本実施例では、送受信者が同じでも鍵生成・選択装置１３の初期値を利用する毎に変更するようにして安全性を向上させるようにしている。

【００９４】実施例６に示された鍵列生成の手順である式（７）、式（８）において、フィードバック演算により次々更新されるx_{ji}を、鍵生成・選択装置１３の内部変数と呼ぶことにする。本実施例の鍵生成・選択装置１３は、図１３に示されるように式（７）のフィードバック演算を行う処理回路１３ｈと式（８）の演算を行う処理回路１３ｉと、演算器１３ｊとから構成され、さらに式（７）の演算により更新される内部変数を読み出せる構成になっている。読み出された内部変数は、例えば実施例１で説明したような通信用端末１０に接続された携帯型記憶装置３０の保持手段３０ａに記憶される。

【００９５】実施例６、７では、鍵生成・選択装置１３へ初期値を設定するだけでデータの移動は一方向であるが、本実施例では逆方向に鍵生成・選択装置１３の内部変数の読み出しが行えるようになっている。読み出した内部変数は、次回の暗号通信に用いられる共通鍵として、今回の暗号通信に用いた共通鍵に対し置き換えが行われる。

【００９６】また、この鍵生成・選択装置１３を図１０の鍵生成・選択装置１３に置き換えることにより、鍵生成・選択装置１３の初期値を利用する毎に変更できる通信用端末１０を構成できる。

【００９７】加入者ＡからＢへの暗号通信は、実施例６、７で示した手順と同様の手順で行われる。ただし、「鍵を更新しながら暗号化を行う」暗号方式の場合には、送受信者双方に「暗号化データの復号が終了した時

の鍵生成・選択装置の内部変数の値を次回Ａ（又はＢ）と暗号通信するための新しい初期値として携帯型記憶装置の保持手段に秘密に保持する」という手順が最後に必要となる。

【００９８】上述の各実施例は、暗号方式設定信号に基づいていずれかの暗号方式を選択的に用いるように構成される。ここで、上述の暗号方式設定信号は、送信者が任意に選択してもよいし、送信されるデータの種類に応じて自動的にいずれかの暗号方式を選択するようにしてもよい。さらに、送信者が送信内容のセキュリティランクを指定する場合には、指定されたセキュリティランクに応じた強度を有する暗号方式を自動的に設定するようにしてもよい。また、上記暗号方式設定信号は、送信者Ａ、Ｂ間での動作モード、すなわち送信者Ａ、Ｂとの間の通信が、例えばＴＶ会議を行うモードや親展通信を行うモード等、に応じて自動的に暗号強度を変えるようにしてもよい。さらに、上記暗号方式の設定は、データを通信する者が優先的に設定してもよいし、両送信者から自由に設定し得るようにしてもよい。但し、暗号強度を弱くする場合には、相手方の承諾を必要とし、その承諾を得るための交渉を行う通信を行うことが好ましい。また、さらに相手側の復号能力に応じて暗号化方式を設定するようにしてもよい。

【００９９】

【発明の効果】以上説明したように、本発明によれば、暗号通信を行う送受信者の利用する通信手段に、暗号方式を選択できる選択手段を設けることにより、暗号方式を変更できるようにし、さらにその選択した暗号方式を暗号文の送信に先立って送受信者間で共有することにより、従来不可能であった暗号方式の選択を可能にし、自由度の高い暗号通信を可能にしている。

【図面の簡単な説明】

【図１】本発明の実施例１、６による通信用端末のブロック図である。

【図２】本発明の実施例１、６、７による鍵生成・選択装置のブロック図である。

【図３】本発明の実施例１による他の鍵生成・選択装置＊のブロック図である。

【図４】本発明の実施例１～８による携帯型記憶装置のブロック図である。

【図５】本発明の実施例２による通信用端末のブロック図である。

【図６】本発明の実施例３による通信用端末のブロック図である。

【図７】本発明の実施例４による通信用端末のブロック図である。

【図８】本発明の実施例４による暗号装置のブロック図である。

【図９】本発明の実施例５による暗号装置のブロック図である。

【図１０】本発明の実施例６による２乗型疑似乱数を用いた鍵生成・選択装置のブロック図である。

【図１１】本発明の実施例６による鍵更新を行う場合の暗号通信を説明するための構成図である。

【図１２】本発明の実施例７による通信用端末のブロック図である。

【図１３】本発明の実施例８による２乗型疑似乱数を用いた鍵生成・選択装置のブロック図である。

【図１４】共通鍵暗号通信ネットワークの構成図である。

【図１５】公開鍵暗号通信ネットワークの構成図である。

【図１６】共通鍵、公開鍵暗号通信ネットワークの構成図である。

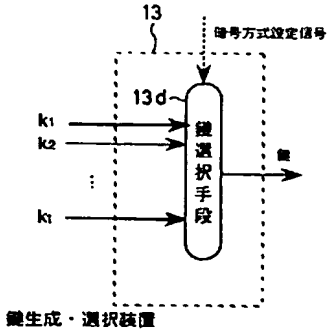
【図１７】従来の通信用端末のブロック図である。

【図１８】ＤＥＳ暗号の１段分の処理を示すブロック図である。

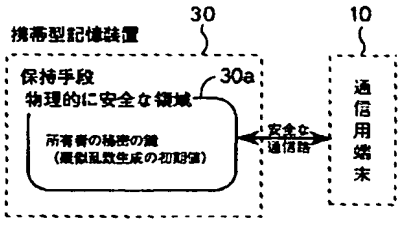
【符号の説明】

１０　通信端末
１１～２０　暗号装置
１２　通信インタフェース
１３　鍵生成・選択装置
１４　選択手段

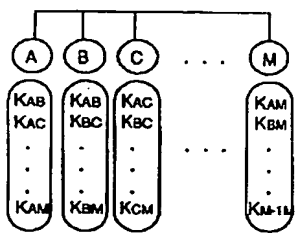
【図３】



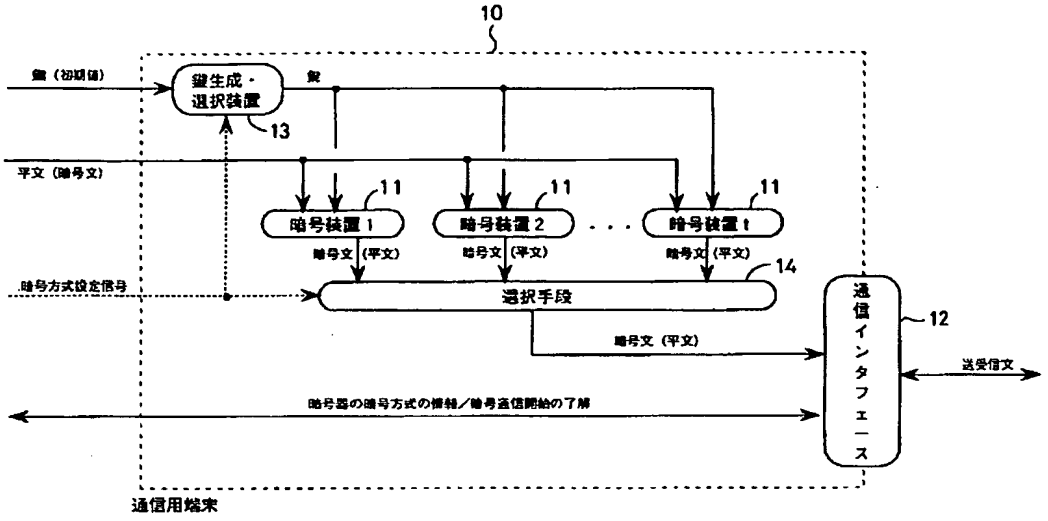
【図４】



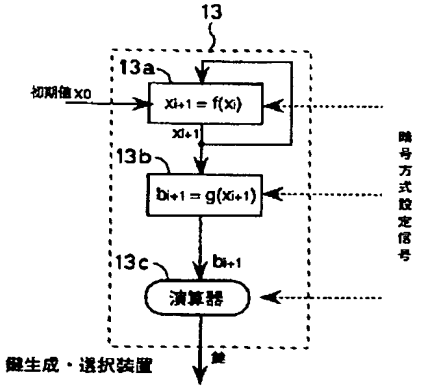
【図１４】



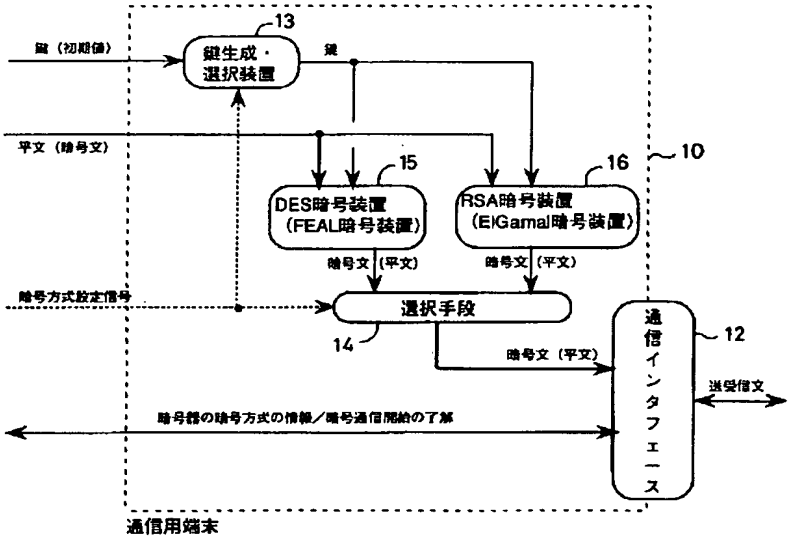
【図１】



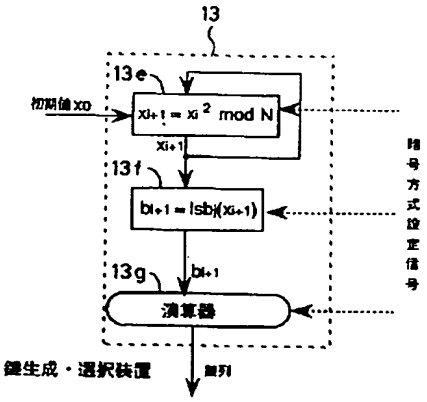
【図２】



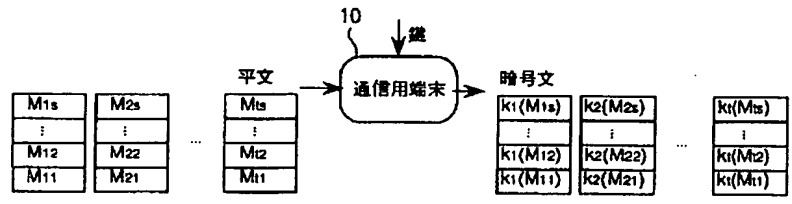
【図５】



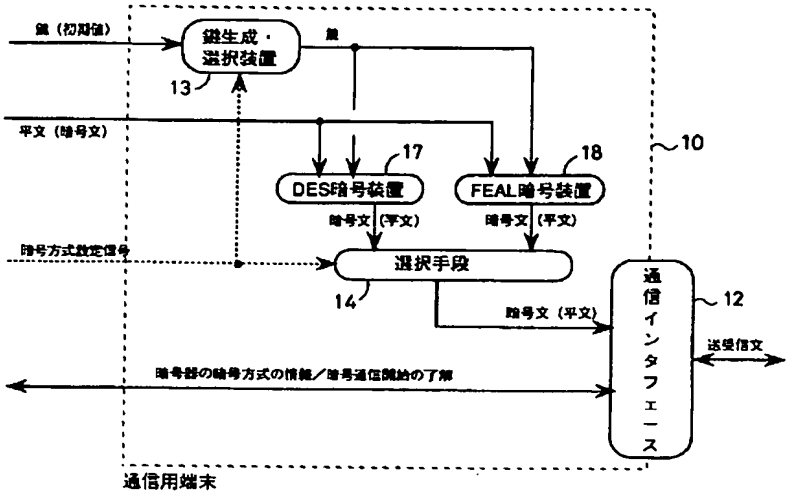
【図１０】



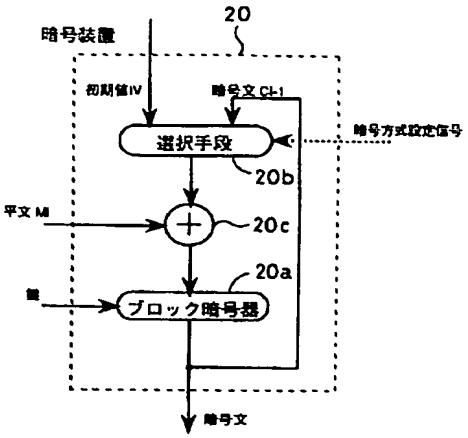
【図１１】



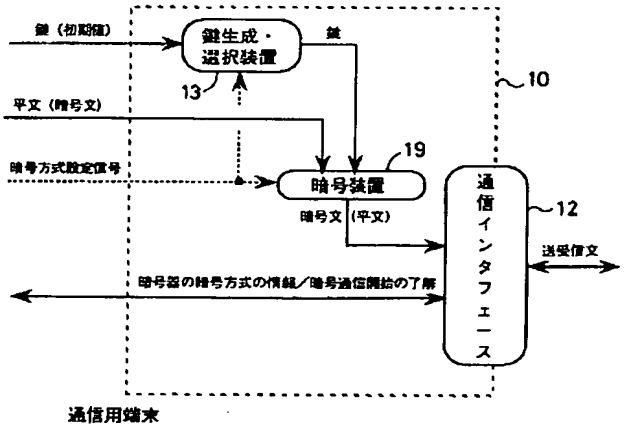
【図６】



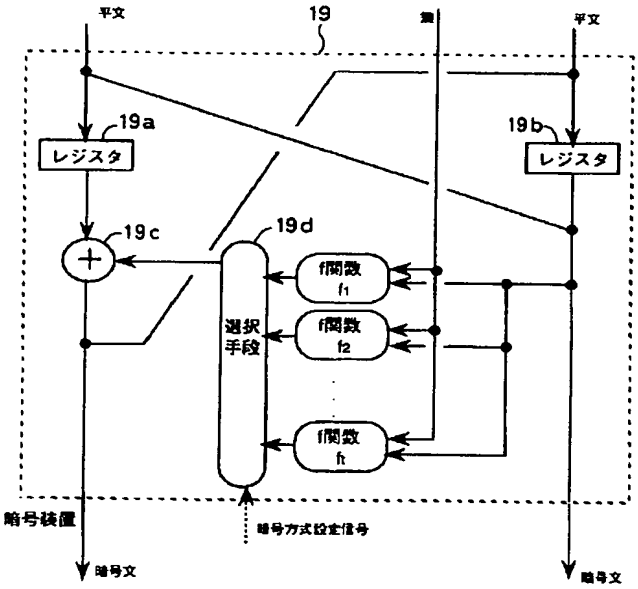
【図９】



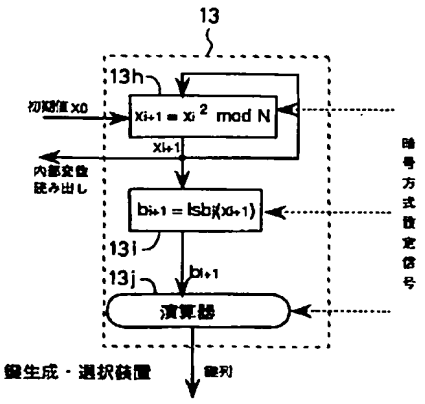
【図７】



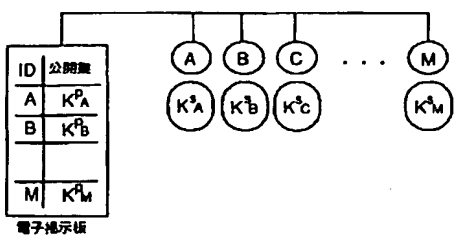
【図８】



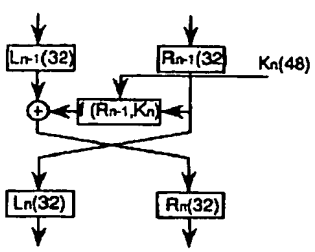
【図１３】



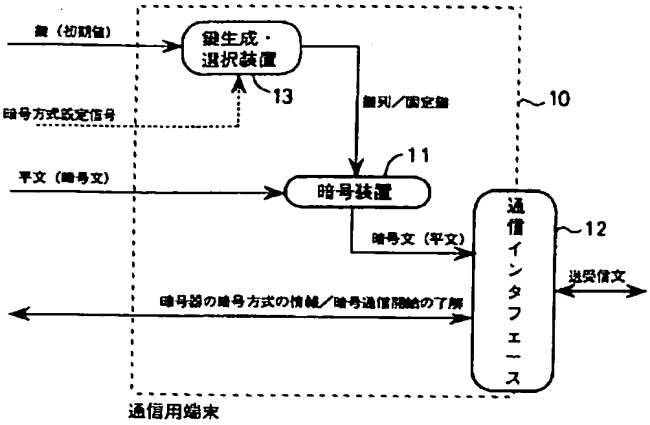
【図１５】



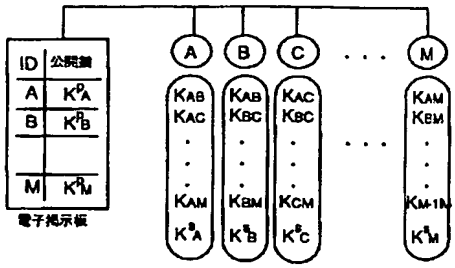
【図１８】



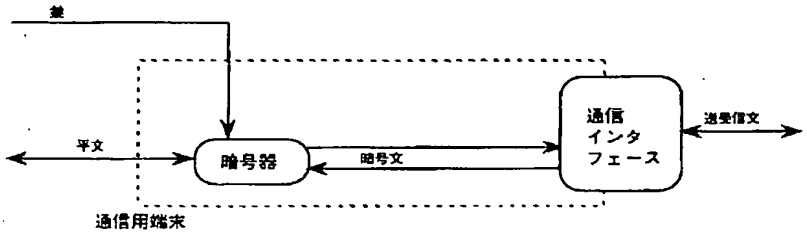
【図１２】


鍵（初期値）
鍵生成・選択装置
13
暗号方式設定信号
鍵列／固定鍵
10
11
平文（暗号文）
暗号装置
暗号文（平文）
通信インタフェース
12
送受信文
暗号器の暗号方式の情報／暗号通信開始の了解
通信用端末

【図１６】


ID
公開鍵
A
B
M
電子掲示板
A
B
C
M

【図１７】


鍵
平文
暗号器
暗号文
通信インタフェース
送受信文
通信用端末